The Office of the National Coordinator for Health Information Technology

# Guide to Privacy and Security of Health Information

Version 1.0 022112

The information contained in this guide is not intended to serve as legal advice nor should it substitute for legal counsel. The guide is not exhaustive, and readers are encouraged to seek additional detailed technical guidance to supplement the information contained herein.

Putting the I in HealthIT

www.HealthIT.gov

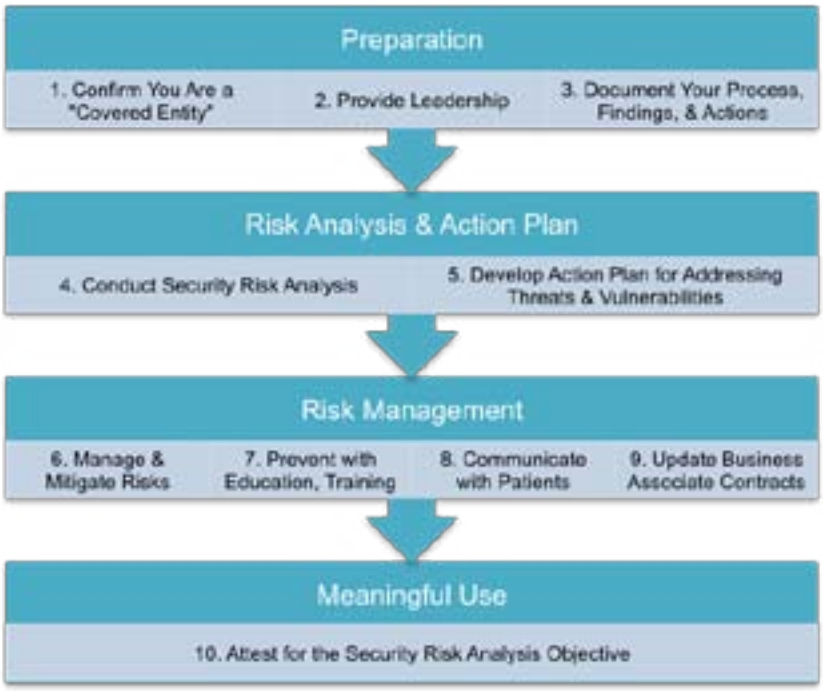
# Chapter 3:

## Privacy & Security 10 Step Plan for Meaningful Use

Before you get started, check with your local Regional Extension Center (REC)[13] about where you can get help beyond the resources in the Privacy and Security Resources section of the website. Work with your electronic health record (EHR) vendor(s) letting them know that health information security is one of your major goals in adopting an EHR. Practice staff and any other partners that you have can also help you fulfill your Health Insurance Portability and Accountability Act of 1996 (HIPAA) responsibilities.

Start your 10-steps at least 90 days before the day you plan to start the EHR incentive program attestation period.

This is not intended as a statement of meeting Meaningful Use (MU) standards; this is one suggested organized process recommended to address the various components.




### Privacy & Security 10-Step Plan for Meaningful Use

#### Step 1: Confirm You Are a "Covered Entity"

Most health care providers are covered entities, and thus, have HIPAA responsibilities for individually identifiable health information. The U.S. Department of Health and Human Services (HHS) tool can help you confirm if you are a covered entity.

#### Step 2: Provide Leadership

Your leadership—especially emphasizing the importance of protecting patient information—is vital to your privacy security activities. For example, HIPAA requires covered providers to designate both a privacy and a security officer on their staff. In a very small practice, you may have to assume both responsibilities.

Your security officer should be able to work effectively with others to safeguard patient information. At various times, the officer will need to coordinate with your privacy officer (if a different person), practice manager, IT administrator or consultant, and your EHR vendor.

13 http://healthit.gov/rec

Subsequent actions are:

- Designate a privacy and security officer. This person will be responsible for developing and maintaining your privacy and security practices to meet HIPAA requirements. This person should be part of your EHR adoption team and be able to work effectively with others. In a very small practice, you may be the privacy and security officer or your practice manager may carry both roles. Be sure to:
  - Record the assignment in a new security documentation file, even if you are the officer.
  - Discuss your expectations and their accountability. Note that you, as a covered health care provider, retain ultimate responsibility for HIPAA compliance.
  - Enable your designated security person to develop a full understanding of the HIPAA Rules so (s)he can succeed in his/her role.
- Explore HIPAA security requirements with your EHR vendor. What security functions does the EHR/Health IT product offer? If you have implemented an EHR, what are the current settings of those functions? What is the vendor's pricing for training staff on those functions, developing relevant policies and procedures, and correcting security-setting deficiencies in the EHR system?
- Select a qualified professional to assist you with the security risk analysis. Your security risk analysis must be done well or you will lack the information necessary to effectively protect patient information. Note that doing the analysis in-house may require an upfront investment developing a staff member's knowledge of HIPAA and electronic information security issues. Use this opportunity to have your staff learn as much as possible about health information security.

  You however, can conduct the risk analysis yourself. Just as you contract with professionals for accounting, taxes, and legal counsel, so, too, outsourcing the security risk analysis function can make sense. RECs often provide this direct support. Another source of assistance may be your state or local medical association, or other professional medical association.

  If you need to, outsource this to a professional, a qualified professional's expertise and focused attention will yield quicker and more reliable results than if your staff does it piecemeal over several months. The professional will suggest cost-effective ways to mitigate risks so you do not have to do the research yourself and evaluate options. You are still ultimately responsible for the security risk analysis even if you outsource this function.

  Talk to several sources of potential assistance. If you contract with a professional, make sure (s)he has both a certification and direct experience tailoring a risk analysis to medical practices with a similar size and complexity as yours.
- Use a checklist as a security risk preview. Have your security officer or security risk professional performing the risk analysis use a checklist to get a preliminary sense of potential shortcomings in how your practice protects patient information. A single checklist does not fulfill the security risk analysis requirement, but the checklist will help everyone get ready for needed improvements.

  Keep the results as part of your documentation (see Step 3).
- Continue to refresh your knowledge base. Learn about HIPAA, state laws, and other privacy and security

requirements that also require compliance.

- Promote culture of protecting patient privacy. "Culture" means creating an overall atmosphere in your office that is protective of patients' information. Culture sets the tone.
    - Constantly communicate through your actions as you comply with, implement, and enforce your privacy and security policies and procedures. Second, remind staff why securing patient information is important to patients and the medical practice.

Over time, protecting privacy will become ingrained into all aspects of your practice operations. Further, your patients will feel and sense that you are safeguarding their health information.

## Where to Find Help

### Your local REC may offer:

- Direct support with conducting the security risk analysis, training staff, and risk mitigation.
- Guidance, information resources, and tools.
- A list of professionals qualified to conduct security risk analyses.

Also, your REC or your membership associations may know of training resources. Training may be available through your local community college.

The Privacy and Security Resources page provides some useful education materials.

## Certification in Health Information Security

### Two examples of certification are:

- Certified in Healthcare Privacy and Security (CHPS)
- Certified Professional in Healthcare Information and Management Systems (CPHIMS)

## Step 3: Document Your Process, Findings, and Actions

The Centers for Medicare & Medicaid Services (CMS) within HHS advise all providers that attest for the EHR incentive programs to retain all relevant records that support attestation. Thus, faithfully record all your practice decisions, findings, and actions related to safeguarding patient information. These records will be essential if you ever are audited for compliance with HIPAA[14] or an EHR incentive program.

Documentation shows why and where you have security measures in place, how you created them, and what you do to monitor them. Create a paper or electronic folder for your records.

The HHS Office for Civil Rights (OCR) and state attorneys general investigate HIPAA complaints; OCR conducts audits[15] for HIPAA privacy and security rule compliance. Providers in the CMS EHR incentive programs may also receive a random audit from CMS to determine if they actually conducted the security risk analysis and implemented adequate safeguards.

Records about how you did the security risk analysis and acted on the results would inform an audit.

### Examples of Records for Your Privacy and Security Documentation Folder

Contents should include, but not be limited to:

- Completed checklists
- Security risk analysis report
- Risk management action plan
- Agreements for business associates
- Trainings for staff and any associated certificates
- EHR logs that show utilization of security features and monitor user actions
- Your policies and procedures

Also, this documentation should help you run your practice efficiently. You will eventually have a master record of security findings, decisions, and actions that your workforce can reference instead of trying to reconstruct from memory and scattered bits of information.

## Step 4: Conduct Security Risk Analysis

Conduct a security risk analysis (or reassessment if you already conducted a risk analysis) that compares your current security measures to what is legally and pragmatically required to safeguard patient information. The risk analysis also identifies high priority threats and vulnerabilities.

OCR has issued Guidance on Risk Analysis[16] , and in conjunction with the U.S. Department of Health and Human Services Office of the National Coordinator for Health Information Technology (ONC), a security risk assessment tool . ONC offers a set of questions tailored to small practices that can help you get started on a risk analysis. A security risk professional can plan and implement this process, but you will want to know what to expect.

14 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html
15 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html
16 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html

The first time you conduct a risk analysis:

- Review the existing security infrastructure in your medical practice against legal requirements and industry best practices. An optional analysis is to assess how well your medical practice currently fulfills nationally accepted principles for data stewardship.
- Identify potential threats to patient privacy and security vulnerabilities and assesses the potential impact if that what-if occurred.
- Prioritize risks for action based on the likelihood of specific risks and their potential impacts on patients, the practice, and others.

Follow a specific process in conducting the risk analysis so that you consider all potential threats and vulnerabilities. The process does not need to be formal (e.g., that you used a specific tool), but it should be systematically approached so it covers all security risks.

Make sure your risk analysis examines risks specific to your situation, including if your EHR is based in your office or Internet-based. The latter you may also know as "cloud computing" or "application service provider (ASP).

Free do-it-yourself tools for the security risk analysis

## What to Expect

- Each step will require bringing your security team together and deciding who will be responsible for what component.
- You will finish the risk analysis, but then need to use the information to create and implement an action plan.
- Periodically – at least annually – you will need to return to the risk analysis report and reassess.
- The risk analysis can produce murky results. However, you will be able to see where you are meeting, not meeting, or exceeding HIPAA requirements.
- The risk analysis process is ongoing. There is no simple checklist that you can use to know that your security process is "done" or sufficient.
- Federal, state, and privacy and security requirements will continue to evolve.

## Security Risks in Office-Based vs. Internet-Hosted EHRs

Both office-based (locally-hosted) and Internet-hosted (remotely-hosted) EHRs have features that enable your practice to better control access to and use of protected health information than was available with paper medical records. On the other hand, both EHR types also introduce new risks to your patients' information. The mix of security risks relates, in part, to your EHR type.

The table on the next page offers a few examples of different risks associated with office-based vs. Internet-hosted EHRs(CPHIMS).

| Examples of Potential Information Security Risks with Different EHR Hosts | |
|---|---|
| Office-Based EHRs | Internet-Hosted EHR |
| Natural disaster could greatly disrupt availability of, and even destroy, protected health information. | The vendor controls many security settings, the adequacy of which may be hard to assess. |
| The security features on your office-based EHR may be less sophisticated than an Internet-hosted EHR. | Your data may be stored outside the U.S. Other countries have different health information privacy & security laws. |
| You directly control the security settings. | You are more dependent on the reliability of your Internet connection. |
| When public and private information security requirements change, you have to figure out how to update your EHR to comply and work out any bugs. | In the future, the vendor might request extra fees to update your EHR for compliance as federal, state, and private information security requirements evolve |

are available on the Privacy and Security Resources page, and some RECs[17] provide this service or can provide additional tools. Look for tools that are suitable to your practice in terms of scale and terminology. Some commercial security risk analysis products are now available; before buying one, seek out an independent review from a health information security expert. Be sure to involve your EHR vendor, beginning with some basic questions.

For Meaningful Use purposes, a risk analysis only need to be done once per year or when a major change occurs to your practice or electronic system, such as your decision to participate in a health information exchange (HIE)[18]. Annual reassessments will take less time and effort than the original full risk analysis. Review and update the prior analysis for changes in risks.

## Step 5: Develop an Action Plan

Using your risk analysis results, discuss and develop an action plan to mitigate the identified risks. The plan must have five components: administrative, physical, and technical safeguards; policies and procedures; and organizational standards. Often, basic security measures can be highly effective and affordable.

Your action plan is informed by your risk analysis and should focus on high priority threats. Take advantage of the flexibility that you have to right-size security measures to your specific practice characteristics. It is important that your security be right-sized so the plan is feasible and affordable for your practice.

Your action plan should have at least any combination of the five required components, which are addressed in Steps 3 and 6-9. Although the steps are sequential, the security components are interrelated. Begin with identifying the easy actions that can reduce the greatest risks.

To develop your action plan, your staff that has been designated as being responsible for security should schedule time together to prioritize actions and structure into steps. Once the plan is written, your designated security staff will need to

17 http://www.healthit.gov/rec
18 http://healthit.hhs.gov/portal/server.pt?open=512&objID=1488&mode=2

continue to meet periodically to coordinate actions, work through unexpected snags, and track progress. If your staff is unsure of how a specific HIPAA requirement might apply to your specific practice, review OCR specific guidance or other materials in the Privacy and Security Resources. Also, you could seek guidance from your legal counsel or a security risk professional.

Last but not least, reward your team as it achieves milestones. Also, understand that you will not be able to eliminate risk, but you will be able to lower it.

### Step 6: Manage and Mitigate Risks

Begin implementing your action plan. Develop written and up-to-date policies and procedures about how your practice protects e-PHI. Retain outdated policies and procedures. Do not lose sight of basic security measures, some of which can be low-cost and highly effective

Your EHR vendor can help you use the security functions in your certified EHR[19].

This step is focused on implementing your action plan, especially three parts:

- Information security settings in your EHR
- Written policies and procedures
- Continuous monitoring of your security infrastructure

The goal is to protect patient information through ongoing efforts to identify, assess, and manage risks.

## Remember the Basics

- Is your server in a room only accessible by authorized staff? Do you keep the door locked?
- Are your passwords easily found (e.g., taped to a monitor)? Easy to guess?
- Do you have a fire extinguisher that works?
- Where, when, and how often do you back-up? Is at least one back-up kept offsite? Can your data be recovered from the back-ups?
- How often is your EHR server checked for viruses?
- Who has keys to your building? Any former employees or contractors?
- What is your plan for what to do if your server crashes and you cannot directly recover data? Do you have documentation about what kind of server it was, what software it used, etc.?
- If your practice manager takes a break, would his/her screen still display patient data?

19 frrn8--fc_jrfgr,ffq,emt-AFNJ,

Above all, integrate information security into your practice routines and create a culture of continually safeguarding patient information.

### Information Security Settings in Your EHR

A certified EHR assures that your new system has a package of core technical security functions[20] However:

- Certification does not guarantee performance or reliability of these security functions.
- The security functions may be "off" or the settings could be at a suboptimal level, either of which can create vulnerabilities.
- You and your staff should become familiar with the security settings in your EHR. Most of these are accessible to whoever has administrator privileges. Learning how to configure these settings, for example, will help when staff leave or join your practice. While nationally accepted standards on these configurations have not yet been developed, there are industry best practices. Your health information organization that facilitates electronic exchanges may have specific requirements.
- Your risk analysis should specifically examine the adequacy of your EHR security safeguards as it transmits, stores, and allows modifications to protected health information.
- You may need to contract with an information security expert at some point but you should first avail yourself of other sources, such as the REC for your area, Privacy & Security Resources, your EHR vendor, or your state or county medical association. These resources can assist you in assuring that your EHR security features are appropriately configured.

### Written Policies and Procedures

Your policies and procedures guide how your practice operates on a day-to-day basis with respect to protecting patient information. HIPAA requires these to be written. Your REC consultant may have a sample manual.

To use as a guide, your medical practice policies and procedures should at least:

- Establish protocols for all of your security components (administrative, physical, and technical safeguards).
- Recognize individual privacy rights and specify processes for fulfilling these responsibilities.
- Instruct your workforce on what to do when something happens that impairs the availability, integrity, or confidentiality of protected health information. (Sometimes called incident response or management plans.)
- Specify a process and sanctions for breach notification.
- Detail enforcement, starting with the use of your EHR security logs to monitor access to and use of protected health information. Breach notification policy violations must have sanctions.

Once your written policies and procedures are in place, HIPAA requires that you:

20 https://www.cms.gov/EHRIncentivePrograms/Downloads/EP-MU-TOC.pdf,

- Train staff (see Step 7) on what is required and how to implement the policies and procedures. HIPAA requires that your workforce be specifically trained on your medical practice's policies and procedures for breach notification.
- Consistently apply the policies and procedures when unauthorized access occurs. Make sure your staff is aware of related enforcement. Staff members who do not comply with your breach notification must be sanctioned. Document your actions.
- Periodically review your policies and make sure they are still current and your practice is adhering to them.
- Update your policy and procedures when your internal or external environment changes, creating new risks.
- Retain policies and procedures for six years after you have updated or replaced them. State and private requirements may specify a longer time period.

### Continuous Monitoring of Your Security Infrastructure

In the security risk analysis illustration (see Chapter 3, or download the entire guide here) the "monitor results" is the process of reviewing how well your security infrastructure works. The security risk analysis provides feedback that your practice needs for continuous improvement, documentation, and your annual analysis of security risks.

Monitoring results also relates to a HIPAA Security Rule requirement that you have audit controls and the capability to audit. Your audit controls and capabilities should be in scale with the size of your practice. (Note: in this context, "audit" is what you do to monitor the adequacy and effectiveness of your security infrastructure and make needed changes.)

Your certified EHR has a function to generate audit logs. This means it can record how protected health information is accessed, by whom, what the individual did, when, and for what purposes. Your EHR also can produce reports. Audit logs are useful tools for both holding your workforce accountable for protecting patient information and for learning about unexpected or improper modifications to patient information.

Have your security officer, IT administrator, and EHR vendor work together so your audit function is active and configured to your needs. They may want you to:

- Decide whether you will conduct the audits in-house, by an information security consultant, or a combination of the two.
- Determine what to audit and how the audit process will occur.
- Identify trigger indicators—or signs that protected health information could have been compromised and further investigation is needed.
- Establish a schedule for routine audits and guidelines for random audits.

## Step 7: Prevent with Education and Training

To safeguard patient information, your workforce must know how to implement your policies, procedures, and security audits. HIPAA requires you as a covered provider to train your workforce (employees, volunteers, trainees, and contractors serving on your workforce) on your policies and procedures. Your staff must receive formal training on breach notification.

Reinforce workforce training with reminders. Lead by example in adhering to your policies and procedures.

Workforce education and training—plus a culture that values patients' privacy—are a necessary part of risk management.

### Workforce Education and Training

You need your staff to adhere to your security policies and procedures and understand their roles and the potential consequences of not adhering to them. Your staff may need focused training to develop the requisite skills to perform the steps required.

Breach notification is a training component that HIPAA specifically requires.

### How Often?

HIPAA requires your practice to formally educate and train your workforce at least once a year and when your practice changes policies or procedures.

### Make Protecting Patient Information Part of Your Routine

Deliberately create an operational culture that emphasizes patient confidentiality. Lead by example by complying with your practice policies and procedures. Speak often about the importance of trust in the patient-provider relationship and that patients expect your practice to be a good steward of their health information. Also:

- Continually remind staff to safeguard patient confidentiality and the security of protected health information.
- Make sure your staff has a copy of your policies and procedures for easy reference.
- Address staff questions.
- Reassess each workforce member's job functions and enable him/her to access only the minimum necessary health information as appropriate.

## Step 8: Communicate with Patients

Your patients may be concerned about confidentiality and security of their health information in an EHR. Emphasize the benefits of EHRs to them as patients, perhaps using consumer education handouts that others have developed. Reassure them that you have a system to proactively protect their health information privacy. Good patient relations also mean you have policies and procedures for communicating with patients and caregivers if a breach of unsecured protected health information (PHI) occurs.

Most patients trust their providers to keep their health information confidential, but some patients may worry about their privacy being compromised in EHRs and electronic sharing of their health information.

Don't surprise patients with your EHR adoption; instead, develop a four-part effort to:

- Communicate with patients about the security and confidentiality of their health information. This includes, but goes beyond your Notice of Privacy Practices.[21]

21 http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/notice.html

- Address their individual health information rights, especially the right to access a copy of their electronic medical record.
- Educate patients about how their health information is used and may be shared outside your practice. In some cases, depending on state law and the nature of information you are sharing, you may need to obtain a patient's authorization or permission prior to exchanging their health information.
- Notify patients and caregivers when a breach of unsecured PHI has occurred (this is referred to as a breach notification), following your previously developed policies and procedures.

Patient relations on privacy and security issues should be an integral part of your overall patient engagement strategy.[22]

Consumer communications should be culturally appropriate. Consider language, communication needs, and the level of trust that seems to exist between different patient populations and health care providers. If a population has some distrust of the medical establishment, then take extra steps to reassure them that you are safeguarding their information.

For concerned patients and their caregivers, be ready to guide them through the change. For ideas, see the Privacy & Security Informational Resources, which provides other materials for you and your patients.

Fulfill Your Responsibilities for Patients' Health Information Rights

In the future, expect more patients to ask how you handle their electronic health information. More patients will ask for their medical records, and some will want changes to their records.

To prepare for patient requests, ask your EHR vendor and REC consultant about ways to use your system to help you fulfill individual patient rights. A good place to start is focusing on the EHR incentive program objective of giving patients a copy of their electronic health information upon request. For example, walk through the steps of saving a patient's record on a mobile device such as a disc or jump/USB drive (which should be password protected or encrypted) as well as how to print out a patient's record. Ask your vendor to provide step-by-step instructions that include screen shots on how to perform these actions.

Once you have established a process and procedure on how patients can get a copy of their EHR, develop procedures for patients to ask you to modify their health information, restrict disclosure, and obtain a report about prior disclosures. (Patients' Individual Rights and Your Responsibilities section explains these legal rights.)

Online Communications with Patients

If you plan to interact with patients via online platforms (e.g., e-mail, a patient portal for your EHR, or social media) adhere to HIPAA requirements for protected health information. Check the Privacy & Security Resources page for more information.

## Step 9: Update Business Associate Agreements

Make sure your business associate[23] agreements require compliance with HIPAA and Health Information Technology for Economic and Clinical Health Act (HITECH) Breach Notification requirements. This will require your business associates to safeguard protected health information they get from your practice, train their workforce, and adhere to breach notification

22 http://www.healthit.gov/patients-families
23 http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html

requirements. OCR offers a sample business associate contract provisions[24].

Health information organizations (HIOs) that facilitate the electronic exchange of individual patient information may also be considered business associates. Please see OCR's guidance pertaining to HIO[25].

If you electronically exchange protected health information with others, be sure your agreement with your health information organization is also up to date.

Organizational standards are a required HIPAA security component. First, make sure your written policies require all business associates that routinely access protected health information to comply with HIPAA and HITECH, including breach notification. These policies should also state how business associates are accountable. Next, update your agreements with your business associates to be compliant with existing and new standards.

## Step 10: Attest for the Security Risk Analysis MU Objective

Only apply for an EHR incentive program, after you have fulfilled the security risk analysis requirement and have documented your efforts.

Do not register and attest for an EHR Incentive program[26] until you have conducted your security risk analysis (or reassessment) and corrected any deficiencies identified during the risk analysis. Document these changes.

When you attest to meaningful use, it is a legal statement that you have met specific standards, including that you protect electronic health information. Providers participating in the EHR Incentive Program can be audited.

If you attest prior to actually meeting the meaningful use security requirement, you could increase your business liability for federal law violations and making a false claim. From this perspective, consider implementing multiple security measures as feasible, prior to attesting. The priority would be mitigating high-impact and high-likelihood risks.

24 http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html
25 http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html
26 Centers for Medicare and Medicaid Services. Eligible Professional Meaningful Use Core Measures. Measure 15 of 15. Nov. 7, 2010. Available at: http://www.cms.gov/EHRIncentivePrograms/Downloads/15ProtectElectronicHealthInformation.pdf